CHARACTERISTIC AND MINIMAL POLYNOMIALS OF LINEAR CELLULAR AUTOMATA

DIANA M. THOMAS, JOHN G. STEVENS AND STEVEN LETTIERI

DEPARTMENT OF MATHEMATICAL SCIENCES

MONTCLAIR STATE UNIVERSITY

UPPER MONTCLAIR, NJ 07043

Abstract. The 1984 article by Martin, Odlyzko and Wolfram on Wolfram's Rule 90 heightened interest in the area of linear cellular automata defined on a vector space over a finite field [6]. In this article we find the closed form expression for the minimal polynomial of Rule 90, which is then used to completely characterize the dynamics of the map. In addition, we show that the standard basis vectors in $\mathbb{Z}_2^n$ lead to the maximal cycle for any linear finite dimensional cellular automata with periodic boundary conditions. Finally, we address questions posed by Tadaki on the connection between Rule 90 and Rule 150.

1. Introduction

A finite dimensional cellular automaton (CA) is a discrete time dynamical system defined on a finite dimensional vector space for which the next state is updated by a local deterministic rule. Each component in the vector space is considered as a cell typically taking on only two values, 0 and 1. If the vector space is defined over a finite field, all forward orbits of a CA converge to a periodic cycle in finite time. Therefore, for finite dimensional CA, the main problem under consideration is determining the transient behavior and cycle lengths of the map.

In the case of a CA defined over a finite dimensional string taking on values from $\{0, 1\}$, an important distinction is whether the update map acts linearly when the state space is viewed as a vector space over $\mathbb{Z}_2$. In such a setting, one can exploit the algebraic structure of a vector space over a finite field and apply the many known results of iteration of linear maps.

The concept of CA as a dynamical system on a vector space over a finite field was employed by Martin, Odlyzko and Wolfram in their 1984 paper [6] on Wolfram's Rule 90 given by:

$$W_n \mathbf{x} = (x_n + x_2, x_1 + x_3, \ldots, x_{n-1} + x_1) \tag{1}$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$ and the addition is modulo 2. Since 1984, many articles have appeared extending and generalizing the results in [6] to other linear rules [4,5,8,9]. The focus of the research on W_n and its extensions involved characterizing and predicting the cycle lengths of the linear CA by utilizing the finite field structure.

E. Jen characterized limit cycle structure through orders of minimal polynomials in the cylindrical case. Stevens proved that all cycle length for any finite dimensional linear CA can be obtained as orders of minimal annihilating polynomials [9]. Moreover, the transient behavior can be obtained from the number of factors of λ belonging to the minimal polynomial.

In two articles [10,11], Tadaki uses a recursion equation to find the characteristic polynomial of Rule 150 and connect the cyclic behavior to Rule 90. However, as stated earlier, period lengths are not obtained through the characteristic polynomial, but through the minimal polynomial. To this end, this paper restates the proof that all period lengths are equal to orders of factors of the minimal polynomial of the map. In Section 3, we find a closed form expression for the minimal polynomial of Rule 90 using a dimensional and symmetry argument. Several observations on Rule 90 are direct results of the proof of this theorem. Section 4 discusses Rule 150 and its connection to Rule 90. Data on all periods up to $n = 40$ for Rules 90 and 150 are provided. Some general problems for further work are suggested in Section 5.

2. CHARACTERIZATION OF CYCLE LENGTHS AS ORDERS OF MINIMAL ANNIHILATING POLYNOMIALS

Although the results in this section are posed over $\mathbb{Z}_2^n$ due to the present applications, all results hold for any generalized finite field with characteristic p. The following definitions are used extensively in our analysis.

Definition 2.1. The *minimal annihilating polynomial* of a vector $\mathbf{v} \in \mathbb{Z}_2^n$ is the monic polynomial $\mu_v(\lambda)$ of least degree such that $\mu_v(A)\mathbf{v} = 0$.

The existence of such a polynomial is guaranteed by the Cayley-Hamilton theorem which states that the characteristic polynomial of A will annihilate A.

Definition 2.2. Let $q(\lambda)$ be a polynomial with coefficients in $\mathbb{Z}_2$. Suppose that $q(0) \neq 0$. Then the *order of* $q(\lambda)$, $\mathrm{ord}(q(\lambda))$, is defined to be the smallest natural number, c, such that $q(\lambda)|\lambda^c - 1$. If $q(0) = 0$, then $q(\lambda)$ can be written as $\lambda^k \tilde{q}(\lambda)$, for some positive integer k, where the polynomial, $\tilde{q}(\lambda)$, has the property, $\tilde{q}(0) \neq 0$. In this case, the order of $q(\lambda)$ is defined to be the order of $\tilde{q}(\lambda)$.

The characterization result that identifies transient behavior and cycle lengths follows:

Theorem 2.1. *Let* $\mathbf{v} \in \mathbb{Z}_2^n$. *Let* $\mu_v(\lambda)$ *be the minimal annihilating polynomial of* $\mathbf{v}$. *Assume that* $\mu_v(\lambda) = \lambda^k \tilde{\mu_v}(\lambda)$ *where* $k \geq 0$ *and* $\tilde{\mu_v}(\lambda)$ *is a monic polynomial with* $\tilde{\mu_v}(0) \neq 0$. *Then the* k^{th} *iterate of* $\mathbf{v}$ *belongs to a periodic cycle with period length* $c = ord(\mu_v)$.

A variation of this characterization result first appeared in [5]. We restate the proof of this theorem that can be found in [9].

Proof:

Let $A^j\mathbf{v}$ be the first iterate that belongs to the periodic cycle. Denote the minimal length of the cycle by c. Then $A^c(A^j\mathbf{v}) = A^j\mathbf{v}$, so $A^j(A^c - I)\mathbf{v} = 0$. Since the minimal annihilating polynomial divides any other annihilating polynomial of $\mathbf{v}$ we know that, $\mu_v(\lambda)|\lambda^j(\lambda^c - 1)$.

This means that $\lambda^k|\lambda^j$ and $\tilde{\mu_v}(\lambda)|\lambda^c - 1$. Therefore, $\mathrm{ord}(\tilde{\mu_v}(\lambda)) \leq c$.

Now we will show that $\text{ord}(\tilde{\mu_v}(\lambda)) = c$. Assume on the contrary that $\text{ord}(\tilde{\mu_v}(\lambda)) = l < c$. Then $\tilde{\mu_v}(\lambda)|\lambda^l - 1$, $\lambda^k(\lambda^l - 1) = \mu_v(\lambda)q(\lambda)$ for some q. Therefore $A^k(A^l - I)\mathbf{v} = \mu_v(A)q(A)\mathbf{v} = q(A)\mu_v(A)(\mathbf{v}) = 0$, which means that $A^l A^k \mathbf{v} = A^k\mathbf{v}$. Therefore, $A^k\mathbf{v}$ is on a periodic cycle of length $l < c$. This is a contradiction to the minimality of c.

Now we will show that $k = j$. Recall that $A^j\mathbf{v}$ was first iterate on cycle and $\mu_v(\lambda) = \lambda^k \tilde{\mu_v}(\lambda)$.

Because $\lambda^k|\lambda^j$ it follows that $k \leq j$. Assume on the contrary that $k < j$.

Given that $\tilde{\mu_v}(\lambda)|\lambda^c - 1$, we have $\mu_v(\lambda)|\lambda^k(\lambda^c - 1)$. This implies $\lambda^k(\lambda^c - 1) = \mu_v(\lambda)p(\lambda)$, for some polynomial p. Therefore, $A^k(A^c - 1)\mathbf{v} = p(A)\mu_v(A)\mathbf{v} = 0$. Hence, $A^c(A^k\mathbf{v}) = A^k\mathbf{v}$, which implies that $A^k\mathbf{v}$ is on the periodic cycle. Recall that $A^j(\mathbf{v})$ is *first* iterate to be on the cycle and so we arrive at a contradiction. ■

The minimal annihilating polynomial for any given $\mathbf{v}$ is a factor of the minimal polynomial. Therefore, all possible period lengths can be obtained from the minimal polynomial of A. Moreover, the maximal period length is equal to the order of the minimal polynomial because there exists a vector whose minimal annihilating polynomial is equal to the minimal polynomial [2].

It is important from a dynamical systems perspective to connect the iterates of a vector $\mathbf{v}$ under A to the minimal annihilating polynomial of $\mathbf{v}$. If $\mathbf{v} \in \mathbb{Z}_2^n$ is a vector contained in a cycle under A, then the *algebraic period* of $\mathbf{v}$ under A is the least positive integer value a such that $A^a v$ is a linear combination of $v, Av, A^2v, \ldots A^{a-1}v$.

If a is the algebraic period of v then we may write

$$A^a v = b_1 v + b_2 A v + \ldots b_{a-1} A^{a-1} v.$$

Then the minimal annihilating polynomial of A is given by

$$\lambda^a - b_{a-1}\lambda^{a-1} - \ldots - b_2\lambda - b_1.$$

Thus, a equals the degree of $\mu_v(\lambda)$. The concept of algebraic period was discussed in [3], although not named as such.

We now use the characterization result to analyze the CA of interest.

3. WOLFRAM'S RULE 90

Wolfram's Rule 90, defined by the map (1) was first studied in the finite field setting in [6]. The map first appears in [7] as a model to predict stunted tree growth in a forest. We now discuss W_n using the language of minimal polynomials.

The matrix representation of W_n in the standard basis is,

$$A_{W,n} = \begin{pmatrix} 0 & 1 & 0 & \ldots & & 0 & 1 \\ 1 & 0 & 1 & 0 & \ldots & & 0 \\ & & & \ddots & & & \\ 0 & & & \ldots & 1 & 0 & 1 \\ 1 & 0 & \ldots & & 0 & 1 & 0 \end{pmatrix}. \tag{2}$$

An algorithm based on Theorem 2.1 was developed in [9] to generate all cycle lengths of a linear CA. Based on this algorithm applied to $A_{W,n}$ cycle lengths up to $n = 40$ were computed and appear in Table 4.

3.1. **The Characteristic Polynomial for Wolfram's Rule 90.**

3.1.1. *The Null Boundary Map.* Wolfram's Rule 90 can be thought of as having periodic boundary conditions or as an infinite sequence on a cylinder. Maps on cylinders have been extensively studied in the literature as in [1,4,5,6,8,9,13]. In an effort to generalize the minimal polynomial result to maps without periodic boundary conditions, Stevens et al. [8, 9] examined the Null Boundary Map, defined by:

$$N_n(\mathbf{x}) = (x_2, x_1 + x_2, x_2 + x_3 + \ldots, x_{n-2} + x_n, x_{n-1})$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$.

The purpose of looking at N_n in this paper is to utilize relationships between the characteristic polynomials of $A_{N,n}$ and $A_{W,n}$ to obtain a closed form expression for the characteristic polynomial of $A_{W,n}$. The following theorem illustrates this connection.

Theorem 3.1. *Let $p_{W,n}(\lambda)$ be the characteristic polynomial for the $n \times n$ matrix A_W and $p_{N,n-1}(\lambda)$ be the characteristic polynomial for the $(n-1)\times(n-1)$ matrix $A_{N,n-1}$. Then $p_{W,n}(\lambda) = \lambda p_{N,n-1}(\lambda)$.*

Proof:

To compute the characteristic polynomial of $A_{W,n}$ we need to calculate the determinant,

$$|A_{W,n} + \lambda I| = \begin{vmatrix} \lambda & 1 & 0 & \dots & & 0 & 0 \\ 1 & \lambda & 1 & 0 & \dots & & 0 \\ & & & \ddots & & & \\ 0 & & & \dots & 1 & \lambda & 1 \\ 1 & 0 & \dots & & 0 & 1 & \lambda \end{vmatrix}. \qquad (3)$$

The determinant expands as

$$M = \lambda |M_{1,1}| + |M_{1,2}| + |M_{1,n}|$$

where $M_{i,j}$ is the $n-1 \times n-1$ minor obtained by eliminating row i and column j from the matrix $A_{W,n} + \lambda I$.

Direct inspection reveals $|M_{1,1}| = \lambda p_{N,n-1}(\lambda)$.

The transpose of $M_{1,2}$ is the matrix

$$M_{1,2}^T = \begin{pmatrix} \lambda & 1 & 0 & \dots & & 0 & 1 \\ 1 & \lambda & 1 & 0\dots & & & 0 \\ & & & \ddots & & & \\ 0 & & & \dots & 1 & \lambda & 1 \\ 0 & 0 & \dots & & 0 & 1 & \lambda \end{pmatrix}.$$

Since, interchanging rows does not change the value of the determinant, we have that

$$\begin{aligned}|M_{1,n}| &= \begin{vmatrix} 1 & \lambda & 1 & 0\ldots & & & 0 \\ & & & \ddots & & & \\ 0 & & & \ldots & 1 & \lambda & 1 \\ 0 & 0 & \ldots & & 0 & 1 & \lambda \\ 1 & 0 & 0 & \ldots & & 0 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & \ldots & & 0 & 1 \\ 1 & \lambda & 1 & 0\ldots & & & 0 \\ & & & \ddots & & & \\ 0 & & & \ldots & 1 & \lambda & 1 \\ 0 & 0 & \ldots & & 0 & 1 & \lambda \end{vmatrix} \\ &= |M_{1,2}^T| = |M_{1,2}|.\end{aligned}$$

Because the computations are over $\mathbb{Z}_2$, $|M_{1,2}| + |M_{1,n}| = 2|M_{1,2}| = 0$. ■

The characteristic polynomial for $A_{N,n}$ was obtained in [8] by applying the method of generating functions to the recursion formula:

$$p_{N,n+1}(\lambda) = \lambda p_{N,n} - p_{N,n-1}.$$

The closed form expression for the characteristic polynomial is given by,

$$p_{N,n}(\lambda) = \sum_{\lceil n/2 \rceil}^{n} \binom{i}{n-i} \lambda^{2i-n} \tag{4}$$

where all the binomial coefficients are to be interpreted modulo 2.

Theorem 3.2. *Let $n = 2k$. Then the characteristic polynomial for $A_{W,n}$ is given by*

$$p_{W,n}(\lambda) = \left(\lambda\left(\binom{k}{k-1} + \binom{k+1}{k-2}\lambda + \binom{k+2}{k-3}\lambda^2 + \ldots + \binom{2k-1}{0}\lambda^{k-1}\right)\right)^2. \tag{5}$$

If $n = 2k+1$ *then*

$$p_{W,n}(\lambda) = \lambda\left(1 + \binom{k+1}{k-1}\lambda + \binom{k+2}{k-2}\lambda^2 + \ldots + \binom{2k}{0}\lambda^k\right)^2. \tag{6}$$

Proof:

The closed form for $p_{W,n}$ is found by obtaining the characteristic polynomial through the relationship formulated in Theorem 3.1 and substituting $n = 2k, 2k+1$ into (4).

The substitution and repeated applications of Kummer's theorem yields,

$$p_{W,n}(\lambda) = \begin{cases} \lambda\left(1 + \binom{k+1}{k-1}\lambda + \binom{k+2}{k-2}\lambda^2 + \ldots + \binom{2k}{0}\lambda^k\right)^2 & \text{if } n = 2k+1 \\ \left(\lambda\left(\binom{k}{k-1} + \binom{k+1}{k-2}\lambda + \binom{k+2}{k-3}\lambda^2 + \ldots + \binom{2k-1}{0}\lambda^{k-1}\right)\right)^2 & \text{if } n \text{ is even.} \end{cases}$$

■

Since the minimal polynomial is a factor of the characteristic polynomial, we will use the characteristic polynomial to arrive at the closed form expression for the minimal polynomial.

3.2. **The minimal polynomial for Wolfram's Rule 90.** The following theorem gives the minimal polynomial for $A_{W,n}$.

Theorem 3.3. *Let* $\mu_{W,n}(\lambda)$ *be the minimal polynomial for the* $n \times n$ *matrix* $A_{W,n}$*. Let* $p_{W,n}$ *be the characteristic polynomial for the* $n \times n$ *matrix* $A_{W,n}$*. Then*

$$\mu_{W,n}(\lambda) = \begin{cases} p_{W,k}(\lambda) & \text{if } n = 2k; \\ \\ \lambda(p_{N,k}(\lambda) - p_{N,k-1}(\lambda)) & \text{if } n = 2k+1. \end{cases} \tag{7}$$

Proof:

Case 1: $n = 2k$

Step 1 Obtain the relationship between $n = 2k$ **and** $n = k$

As stated in Section 3 we know that $p_{W,n}(\lambda) = \lambda p_{N,n-1}(\lambda)$. Furthermore, it was proved in [8] that $p_{N,2k-1} = \lambda p^2_{N,k-1}$. Substituting yields,

$$p_{W,2k}(\lambda) = \lambda^2 p^2_{N,k-1}(\lambda) = p^2_{W,k}(\lambda).$$

Step 2 Verify the structure of the Smith Normal Form of $A_{W,n}$

Because $A_{W,n} - \lambda I$ has an $n-2 \times n-2$ minor with determinant one (Figure 2), we know that the Smith Normal Form has the structure

$$S_n = \begin{pmatrix} 1 & 0 & 0 & \dots & & 0 & 0 \\ 0 & 1 & 0 & 0 & \dots & & 0 \\ & & & \ddots & & & \\ & & & \dots & 1 & 0 & 0 \\ 0 & & & \dots & 0 & r_n(\lambda) & 0 \\ 0 & 0 & \dots & & 0 & 0 & s_n(\lambda) \end{pmatrix} \tag{8}$$

where $r_n(\lambda)s_n(\lambda) = p_{W,n}(\lambda)$, $r_n(\lambda)|s_n(\lambda)$ and $s_n(\lambda) = \mu_{W,n}(\lambda)$.

Step 3 Show $\deg(r_n(\lambda)) = \deg(s_n(\lambda)) \leq k$**.**

We will illustrate the concept of our argument by discussing the problem on $\mathbb{Z}_2^6$ first. Consider the basis vector $e_1 = (1, 0, 0, 0, 0, 0)$. Its components can be assigned to the vertices of the polygon having the corresponding number of vertices, as shown in Figure 1. The iterates of e_1 under $A_{W,6}$ are also depicted there. Because $A_{W,n}$ is symmetric, all iterates are symmetric as is evident in Figure 1. Thus, in general, the maximum number of linearly independent iterates of e_1 is k and hence the algebraic period of e_1 is less than or equal to k. Thus, the degree of the minimal annihilating polynomial for e_1 is less than or equal to k.

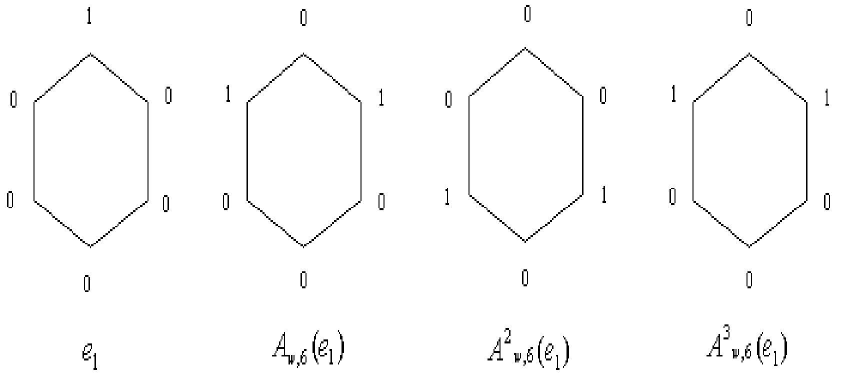

Figure 1. Iterates of $e_1 = (1, 0, 0, 0, 0, 0)$.

We claim that $\mu_{e_1}(\lambda)$ is the minimal polynomial of $A_{W,n}$. To see this first observe that $\mu_{e_1}(\lambda) = \mu_{e_2}(\lambda) = \ldots \mu_{e_n}(\lambda)$. This is true because A_{W_n} commutes with the shift

$$\begin{pmatrix} -\lambda & 1 & 0 & 0\cdots & 0 & 1 \\ 1 & -\lambda & 1 & 0 & 0\cdots & 0 \\ 0 & \ddots & & \ddots & & 0 \\ 0 & 0 & 0\cdots & 1 & -\lambda & 1 \\ 0 & 1 & 0\cdots & 0 & 1 & -\lambda \end{pmatrix}$$

FIGURE 2. Shaded region is a $n-2 \times n-2$ submatrix of $A_{W,n} - \lambda I$ with determinant one.

map:

$$\mu_{e_1}(A_{W,n})e_i = \mu_{e_1}(A_{W,n})S_L^i e_1 = S_L^i \mu_{e_1}(A_{W,n})e_1 = 0.$$

Moreover, if $v \in \mathbb{Z}_2^n$ then $v = \sum_{i=1}^n c_i e_i$ where $c_i \in \mathbb{Z}_2^n$ and $\mu_{e_1}(A_{W,n})v = \sum_{i=1}^n c_i \mu_{e_1}(A_{W,n})e_i = 0$. Therefore $\deg(\mu_{W,n}) \leq k$. This proves that $\deg(s_n) \leq k$. The divisibility condition, $r_n | s_n$, implies the degree of r_n is also less than or equal to k.

Step 4 Show that $r_n(\lambda) = s_n(\lambda)$, which proves that $p_{W,n}(\lambda) = \mu_{A_{W,n}}^2(\lambda)$.

Since $r_n(\lambda)s_n(\lambda) = p_{W,n}(\lambda)$, we know that $\deg(r_n) + \deg(s_n) = 2k$. But since $\deg(r_n) \leq \deg(s_n) \leq k$, this implies that $\deg(r_n) = \deg(s_n) = k$. Since $r_n | s_n$, we have that $r_n(\lambda) = s_n(\lambda)$. Hence, $p_{W,n}(\lambda) = \mu_{A_{W,n}}^2(\lambda) = (p_{W,k}(\lambda))^2$. This proves that $\mu_{W,n}(\lambda) = p_{W,k}(\lambda)$.

Case 2: n=2k+1

The n odd case is proved in a similar fashion as the n even case with minor changes.

If $n = 2k+1$ then from a result in [8],

$$p_{W,2k+1} = \lambda p_{N,2k}(\lambda) = \lambda(p_{N,k}(\lambda) + p_{N,k-1}(\lambda))^2.$$

Let $q_n(\lambda) = p_{N,k}(\lambda) + p_{N,k-1}(\lambda)$.

Step 1 Show $\mu_{W,n}(\lambda)$ has only one factor of λ.

By the closed form expression, (4), $p_{N,2k}(0) = 1$ and $p_{N,2k+1}(0) = 0$. Thus, $q_n(0) = 1$. Therefore, $\lambda | p_{W,n}(\lambda)$, but $\lambda^2 \nmid p_{W,n}(\lambda)$. It follows that $\lambda | s_n(\lambda)$ but $\lambda^2 \nmid s_n(\lambda)$, where $s_n(\lambda)$ is the $(n-1, n-1)$ entry in the Smith Normal Form, (8). Write $s_n(\lambda) = \lambda \tilde{s}_n(\lambda)$.

Step 2 Show $\deg(\mu_{A_{W,n}}(\lambda)) \leq k+1$.

The proof as before uses symmetry arguments to show that $\deg(\mu_{e_1}(\lambda)) \leq k+1$. To see this we need to think of e_1 on a polygon as illustrated in the case $n = 5$ (Figure 3). Due to the symmetry, there can be only at most $k+1$ linearly independent iterates of e_1. Thus the dimension of span$\{e_1, A_{W,n}e_1, \ldots\}$ must be less than or equal to $k+1$. Therefore, $\deg(\mu_{e_1}(\lambda)) \leq k+1$. As in Case 1, μ_{e_1} is the minimal polynomial of $A_{W,n}$

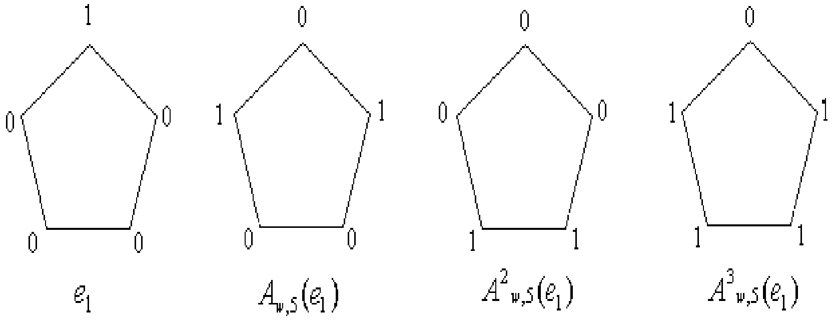

Figure 3. Iterates of $e_1 = (1, 0, 0, 0, 0, 0)$.

and therefore $\deg(\mu_{W,2k+1}) \leq k+1$.

Step 3 Show $p_{W,n}(\lambda) = \lambda(\tilde{s}_n(\lambda))^2$.

We know that $\deg(r_n(\lambda)) \leq \deg(\tilde{s}_n(\lambda)) \leq k$. We also know that $\deg(r_n(\lambda)) + \deg(s_n(\lambda)) + 1 = 2k+1$. This implies $\deg(r_n(\lambda)) = \deg(\tilde{s}_n(\lambda)) = k$. So we can conclude that $r_n(\lambda) = \tilde{s}_n(\lambda)$ and hence, $p_{W,n}(\lambda) = \lambda(s_n^2(\lambda))$ where $s_n(\lambda) = q_n(\lambda)$.

■

A nice result of the above method of proof is that the standard basis vectors in $\mathbb{Z}_2^n$ lead to the maximum cycle for any n. In fact, the basis vectors in $\mathbb{Z}_2^n$ lead to the maximal cycle for any finite dimensional linear CA with periodic boundary conditions. To see this consider the general finite dimensional linear map with periodic boundary conditions:

$$L_n(x) = (a_1x_1+a_2x_2+\ldots+a_nx_1, a_1x_2+\ldots+a_{n-1}x_n, \ldots, a_2x_1+\ldots a_nx_{n-1}+a_1x_n) \quad (9)$$

where $a_i \in \mathbb{Z}_2$ for $i = 1, \ldots, n$. The matrix representation of L_n in the standard basis vectors is the right circulant matrix,

$$A_{L,n} = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & & & a_n \\ a_n & a_1 & a_2 & a_3 & \ldots & & a_{n-1} \\ & & & \ddots & & & \\ a_2 & a_3 & \ldots & & & a_n & a_1 \end{pmatrix}$$

Multiplying $A_{L,n}$ and A_{S_L} where A_{S_L} is the matrix representation of the left shift map verifies that $A_{L,n}$ commutes with A_{S_L}. Commutation with the shift map was the only criteria required to show that $e_i, i = 1, \ldots, n$ led to the maximal cycle under W_n. Thus, the same argument verifies that the basis vectors lead to the maximal cycle under L_n and therefore we can state the following theorem.

Theorem 3.4. *Let L_n be the general linear CA defined in (9). Then the standard basis vectors, $e_i, i = 1, \ldots, n$ lead to the maximal cycle under L_n.*

We now examine Rule 150 and its connection to W_n.

4. Wolfram's Rule 150 and the Banded Map

Wolfram's Rule 150,

$$T_n(\mathbf{x}) = (x_n + x_1 + x_2, x_1 + x_2 + x_3, \ldots, x_{n-1} + x_n + x_1) \tag{10}$$

where $\mathbf{x} = (x_1, x_2, \ldots x_n) \in \mathbb{Z}_2^n$ was studied by Tadaki in [10,11]. In [11], Tadaki arrived at a recursion formula for the characteristic polynomial of $A_{T,n}$. In actuality, Tadaki was working with the null boundary condition map

$$B_n(\mathbf{x}) = (x_1 + x_2, x_1 + x_2 + x_3, \ldots, x_{n-3} + x_{n-2} + x_{n-1}, x_{n-1} + x_n),$$

although not formally stated.

Tadaki's goal was to predict cyclic behavior of Rule 150 by using the closed form expression for the characteristic equation and then to find the relationship between the cycle lengths of Rule 90 and Rule 150. As proved in Theorem 2.1, cyclic behavior is characterized through the minimal polynomial and thus a closed form for the minimal polynomial of $A_{T,n}$ is desired. Because $A_{T,n} = A_{W,n}+I$, the characteristic and minimal polynomials of Rule 150 can be obtained from $p_{W,n}(\lambda)$ and $\mu_{W,n}(\lambda)$. In fact, we have that $p_{T,n}(\lambda) = |A_{W,n}+I-\lambda I| = |A_{W,n}-(\lambda-1)I = p_{W,n}(\lambda+1)$. The same substitution yields $\mu_{T,n}(\lambda) = \mu_{W,n}(\lambda+1)$. This relationship leads to the following result connecting the behavior of both maps.

Theorem 4.1. *If $n = 2^k$, the order of $\mu_{T,n}(\lambda)$ is 2^{k-1}. Furthermore, the order of any minimal annihilating polynomial is 2^j where $j \leq k-1$.*

Proof:

It is shown in [8] that

$$p_{N,2^k-1}(\lambda) = \lambda^{2^k-1}.$$

Therefore,

$$p_{W,2^k} = \lambda^{2^k}.$$

By the closed form expression for the minimal polynomial of $A_{W,n}$ given by, (7),

$$\mu_{W,2^k} = \lambda^{2^{k-1}}.$$

Thus $\mathrm{ord}(\mu_{W,n}(\lambda)) = 1$. From this formulation we have that $\mu_{T,n}(\lambda) = (\lambda+1)^{2^{k-1}}$. The equality implies that $\mathrm{ord}(\mu_{T,n}(\lambda)) = 2^{k-1}$. From the closed form expression, we also can see that $(\lambda+1)^{2^j}$ is a factor of $\mu_{T,n}(\lambda)$ for $j \leq k-1$. Consequently, all

Vector Length	**Cycle Lengths Rule 150**	**Cycle Lengths Rule 90**	**Vector Length**	**Cycle Lengths Rule 150**	**Cycle Lengths Rule 90**
$n = 3$	1	1	$n = 22$	$1, 31, 62$	$1, 31, 62$
$n = 4$	$1, 2$	1	$n = 23$	$1, 2047$	$1, 2047$
$n = 5$	$1, 3$	$1, 3$	$n = 24$	$1, 2, 4$	$1, 2, 4, 8$
$n = 6$	$1, 4$	$1, 2$	$n = 25$	$1, 3, 1023$	$1, 13, 1023$
$n = 7$	$1, 7$	$1, 7$	$n = 26$	$1, 21, 42$	$1, 63, 126$
$n = 8$	$1, 2, 4$	1	$n = 27$	$1, 7, 511$	$1, 7, 511$
$n = 9$	$1, 7$	$1, 7$	$n = 28$	$1, 2, 7, 14, 28$	$1, 7, 14, 28$
$n = 10$	$1, 3, 6$	$1, 3, 6$	$n = 29$	$1, 16383$	$1, 16383$
$n = 11$	$1, 31$	$1, 31$	$n = 30$	$1, 3, 5, 6, 10, 15, 30$	$1, 2, 3, 6, 15, 30$
$n = 12$	$1, 2$	$1, 2, 4$	$n = 31$	$1, 31$	$1, 31$
$n = 13$	$1, 21$	$1, 819$	$n = 32$	$1, 2, 4, 8, 16$	1
$n = 14$	$1, 7, 14$	$1, 7, 14$	$n = 33$	$1, 31$	$1, 31$
$n = 15$	$1, 3, 5, 15$	$1, 3, 15$	$n = 34$	$1, 15, 30$	$1, 5, 10, 15, 30$
$n = 16$	$1, 2, 4, 8$	1	$n = 35$	$1, 3, 7, 21, 4095$	$1, 3, 7, 21, 4095$
$n = 17$	$1, 15$	$1, 5, 15$	$n = 36$	$1, 2, 7, 14, 28$	$1, 2, 4, 7, 14, 28$
$n = 18$	$1, 7, 14$	$1, 2, 7, 14$	$n = 37$	$1, 29127$	$1, 87381$
$n = 19$	$1, 511$	$1, 511$	$n = 38$	$1, 511, 1022$	$1, 511, 1022$
$n = 20$	$1, 2, 3, 6, 12$	$1, 3, 6, 12$	$n = 39$	$1, 21, 4095$	$1, 63, 1365, 4095$
$n = 21$	$1, 7, 63$	$1, 7, 63$	$n = 40$	$1, 2, 3, 4, 6, 12, 24$	$1, 3, 6, 12, 24$

TABLE 1. Period lengths under iterations of the Wolfram's Rule 150 and 90.

minimal annihilating polynomials for $n = 2^k$ must have order 2^j where $j \leq k - 1$.

■

5. CONCLUSION

In this paper, we have obtained closed form expressions for the minimal polynomials of Rule 90 and Rule 150. Since cycle lengths and the transient dynamics can be obtained from the minimal polynomials, such expressions are valuable. Through the computation of the minimal polynomial of Rule 90, we find that the standard basis vectors always lead to the maximal cycle for any finite dimensional linear CA with periodic boundary conditions.

Using the relationship that $\mu_{W,n}(\lambda+1) = \mu_{T,n}(\lambda)$ we obtained connections between the period lengths for both maps when n is a power of two. It would be interesting to investigate further the connection between the order of an arbitrary polynomial, $q(\lambda)$, and the order of $q(\lambda + 1)$.

References

(1) N. Calkin, J. Stevens and D. Thomas, Characterizations of Lengths of Cycles of the N-Number Ducci Game, *Fibonacci Quarterly*, to appear.

(2) Jacobson, N., *Lectures in Abstract Algebra, Volume II-Linear Algebra* (1953).

(3) Lidl R., Niederreiter H., *Finite Fields*, Encyclopedia of Mathematics and its Applications, 20, (1983).

(4) Jen, E., Cylindrical Cellular Automata, *Commun. Math. Phys.*, **119**, 564-590, (1988).

(5) Jen, E., Linear Cellular Automata and Recurring Sequences in Finite Fields, *Commun. Math. Phys.*, **119**, 13-24 (1988).

(6) Martin, O., Odlyzko, Al, Wolfram, S., Algebraic properties of cellular automata, *Commun. Math. Phys.* **93**:219 (1984).

(7) Miller, J.C.P., Periodic forests of stunted trees., *Phil. Trans. R. Soc. Lond.* **A266** p. 63 (1970), **A293** p. 48 (1980).

(8) Stevens, J., Rosensweig, R, and Cerkanowicz, A., Transient and Cyclic Behavior of Cellular Automata with Null Boundary Conditions, *Journal of Stat. Phys*, **73**, 1/2, (1993).

(9) Stevens, John G., On the construction of state diagrams for cellular automata with additive rules., *Information Sciences* 115: 43–59,(1999).

(10) S. Tadaki and S. Matsufuj, Periodicity in One Dimensional Finite Linear Cellular Automata, *Prog. of Theor. Physics*, **89** pp 325-331 (1993).

(11) S. Tadaki, Periodicity in One Dimensional Finite Linear Cellular Automata, *Phys. Rev. E.* **49**, 1168 (1994).

(12) S. Tadaki, Periodicity of cylindrical linear cellular automata, (in review).

(13) F. Vivaldi., Geometry of Linear Maps over Finite Fields, *Nonlinearity* $\underline{5}$: 133-147 (1992).